江苏财经职业技术学院

苏财院〔2021〕91 号

江苏财经职业技术学院
网络安全事件应急预案

1 总则

1.1 编制目的

根据《江苏省网络安全事件应急预案》、教育部《教育系统网络安全应急预案》《江苏省教育系统网络安全事件应急预案》的要求，健全我校校园网络安全应急响应工作机制，规范网络安全事件工作流程，提高我校应对网络安全事件的处置能力，预防和减少网络安全事件造成的损失和危害，确保预防有效、反应及时、处置得当，切实维护学校安全稳定。

1.2 编制依据

《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等法律法规，《国家突发公共事件总体应急预案》《突发事件应急预案管理办法》《国家网络安全事件应急预案》《江苏省实施<中华人民共和国突发公共事件应对法>办法》《江苏省突发公共事件总体应急预案》《教育系统网络安全事件应急预案》《江苏省网络安全事件应急预案》《江苏省教育系统网络安全事件应急预案》《信息安全技术信息安全事件分类分级指南》(GB/Z20986-2007)等文件，以及《江苏财经职业技术学院信息技术安全管理办法》。

1.3 适用范围

本预案适用于学校所有部门单位网络安全事件的应对工作。

按照《江苏省网络安全事件应急预案》《江苏省教育系统网络安全事件应急预案》等规定，本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件（详见附件 1）。其中信息内容安全事件，应同时参照学校有关规定和办法。

1.4 事件分级

参照《江苏省教育系统网络安全事件应急预案》等事件分级规定，结合我校特点，以及网络安全事件可能造成的危害、可能发展蔓延的趋势等，我校网络安全事件分为特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件四级。

（1）符合下列情形之一的，为特别重大网络安全事件（I级）：

①关键信息基础设施或重要信息系统（网站）遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

②关键信息基础设施或重要信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改、假冒，对全省乃至全国教育系统安全稳定和正常秩序构成特别严重威胁。

③网络病毒在全国教育系统大面积爆发并严重影响全省教育系统。

④其他对全省教育系统安全稳定和正常秩序构成特别严重威胁，造成特别严重影响的网络安全事件。

（2）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件（II级）：

①大量省教科网用户无法正常上网。

②关键信息基础设施或重要信息系统（网站）遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

③关键信息基础设施或重要信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改、假冒，对全省教育系统安全稳定和正常秩序构成严重威胁。

④网络病毒在全省教育系统范围内大面积爆发。

⑤其他对全省教育系统安全稳定和正常秩序构成严重威胁，造成严重影响的网络安全事件。

（3）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件（III 级）：

①学校关键信息基础设施或重要信息系统（网站）遭受较大系统损失，造成系统中断，明显影响系统效率，业务处理能力受到严重影响，对全校安全稳定和正常秩序构成较严重威胁。

②学校关键信息基础设施或重要信息系统（网站）的关键数据或重要敏感信息发生丢失或被窃取、篡改、假冒，对全校安全稳定和正常秩序构成较严重威胁。

③网络病毒在全校范围内大面积爆发。

④其他对我校安全稳定和正常秩序构成较大威胁，造成较大影响的网络安全事件。

（4）符合下列情形之一且未达到较大网络安全事件的，为一般网络安全事件（IV 级）：

①校园网某个校区大量用户无法正常上网。

②学校关键信息基础设施或重要信息系统(网站)遭受损失，基本造成系统中断，影响系统效率，业务处理能力受到一定影响，对全校正常秩序构成一定威胁。

③学校重要信息系统（网站）的数据发生丢失或被窃取、篡改、假冒，对全校安全稳定和正常秩序构成一定威胁。

④网络病毒在学校一定范围内广泛传播。

⑤其他对我校安全稳定和正常秩序构成一定威胁，造成一定影响的网络安全事件。

1.5 工作原则

（1）统一指挥、密切协同。学校网络安全与信息化领导小组统筹协调全校网络安全应急指挥工作，建立与省教育厅、淮安市网络安全职能部门、专业机构等多方参与的协调联动机制，加强预防、监测、报告和应急处置等环节的紧密衔接，做到快速响应、正确应对、果断处置。

（2）分级管理、强化责任。按照“谁主管谁负责、谁运维谁负责”的原则，各单位对本单位网络安全工作负主体责任。领导班子主要负责人是网络安全工作第一责任人。

（3）预防为主、平战结合。坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设。提高网络安全事件快速响应和科学处置能力，抓早抓小，争取早发现、早报告、早控制、早解决，严控网络安全事件风险和影响范围。

2 组织机构与职责

2.1 领导机构与职责

网络安全与信息化领导小组统筹协调网络安全事件应急工作，指导我校各部门单位网络安全事件应急处置。当发生特别重大网络安全事件、重大网络安全事件时，在上级统一指挥下开展应急处置工作，具体参照《江苏省教育系统网络安全事件应急预案》等相关规定执行；当发生较大网络安全事件、一般网络安全事件时，成立校网络安全事件应急处置工作组，负责组织和协调事件处置，并根据实际情况吸纳校外相关部门单位和技术支撑单位等参加应对工作。

2.2 办事机构与职责

在学校网络安全和信息化领导小组的领导下，网络安全和信息化领导小组办公室负责网络安全应急管理事务性工作，对接省教育网络安全应急办公室等网络安全职能部门，向学校网络安全和信息化领导小组报告网络安全事件情况，统筹组织学校网络安

全监测工作，指导网络安全支撑单位做好应急处置的技术支撑工作。

2.3 学校各部门单位

学校各部门单位按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，承担各自的网络安全责任，认真做好所建网络和信息系统（网站）的网络安全事件预防、监测、报告和应急工作，并根据本预案制定有关网络和信息系统的网络安全事件专项应急预案，切实落实相关工作责任。

3 监测与预警

3.1 预警分级

建立全校网络安全事件预警制度。按照紧急程度、发展态势和可能造成的危害程度，我校网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生的特别重大、重大、较大和一般网络安全事件。

3.2 安全监测

3.2.1 事件监测

网络安全和信息化领导小组办公室及时传达、监测、发现已经发生的学校网络安全事件，将掌握的情况立即通知相关部门单位。

各部门单位对所建网络和信息系统（网站）的运行状态进行密切监测、一旦发生网络安全事件，立即通过电话等方式向网络

安全和信息化领导小组办公室报告，不得迟报、谎报、瞒报、漏报。

3.2.2 威胁监测

学校接受省教育网络安全应急办组织的全省教育系统网络安全威胁监测。学校通过多种渠道和途径监测、汇聚漏洞、病毒、网络攻击等网络安全威胁信息，依托江苏省教育网络和信息安全通报平台、教育行业漏洞报告平台、教育科研网以及本校漏洞扫描等平台，实现安全威胁信息的收集、校验、发布、跟踪。各部门单位加强对所建网络和信息系统(网站)的网络安全威胁监测，对发现的威胁及时进行处置并上报学校网络安全与信息化领导小组办公室。

3.3 预警研判和发布

学校网络安全与信息化领导小组办公室对监测信息进行研判，对发生网络安全事件的可能性及其可能造成的影响进行分析评估，认为需要立即采取防范措施的及时通知有关部门单位；认为可能发生网络安全事件的信息，应立即向上级报告。如认为可能发生一般网络安全事件，应向学校主要领导和分管领导报告；认为可能发生较大及以上网络安全事件的信息，应向学校网络安全与信息化领导小组报告，经学校网络安全与信息化领导小组批准后，立即向省教育网络安全应急办公室报告。

网络安全与信息化领导小组办公室可根据监测研判情况发布预警或风险提示信息。预警信息包括预警起始时间、可能影响范围、警示事项、应采取的措施、时限要求等。

3.4 预警响应

3.4.1 红色预警和橙色预警响应

根据《江苏省教育系统网络安全事件应急预案》精神，由上级网络安全应急办公室组织红色预警和橙色预警响应工作。

（1）学校网络安全与信息化领导小组办公室根据上级网络安全应急办公室统一部署，组织跟踪和分析研判，密切关注事态发展，做好监测分析和信息搜集工作，研究制定学校防范措施和应急工作方案，协调调度各方资源，做好各项准备工作。重要情况报省教育网络安全应急办公室。

（2）学校网络安全与信息化领导小组办公室及有关单位实行24小时值班，相关人员保持通信联络畅通。

（3）信息化建设管理处技术支撑队伍进入待命状态，检查应急设备、软件工具等，确保其处于良好状态。

3.4.2 黄色预警响应

（1）学校网络安全与信息化领导小组办公室组织预警响应工作。联系有关部门单位、专业机构和专家，研究制订防范措施和应急工作方案，协调调度各种所需资源，做好各项准备工作。

(2)有关部门单位启动专项应急预案,开展预警响应工作,做好风险评估、应急准备和风险控制工作。

(3) 学校网络安全与信息化领导小组办公室及时将事态发展情况向学校网络安全与信息化领导小组报告,经学校网络安全与信息化领导小组批准后，报省教育网络安全应急办公室。

(4) 信息化建设管理处支撑队伍保持联络畅通，检查应急设备、软件工具等，确保其处于良好状态。

3.4.3 蓝色预警响应

(1) 学校网络安全与信息化领导小组办公室组织预警响应工作。联系有关部门单位、专业机构和专家，研究制订防范措施和应急工作方案，协调调度所需资源。

(2)有关部门单位启动专项应急预案,开展预警响应工作,做好风险评估、应急准备和风险控制工作。

(3) 学校网络安全与信息化领导小组办公室及时将事态发展情况向学校主要领导和分管领导报告。

(4) 信息化建设管理处技术支撑队伍保持联络畅通，检查应急设备、软件工具等，确保其处于良好状态。

3.5 预警解除

学校网络安全与信息化领导小组办公室根据上级网络安全应急办公室的通知，及时转发红色预警或橙色预警解除信息。

学校网络安全与信息化领导小组办公室根据实际情况，确定是否解除黄色预警或蓝色预警，及时发布预警解除信息。

4 应急响应

4.1 初步处置

网络安全事件发生后，事发单位应立即启动应急预案，组织本单位的应急队伍和工作人员根据不同的事件类型和事件原因，采取科学有效的应急处置措施，尽最大努力将影响降到最低，并注意保存网络攻击、网络入侵或网络病毒等证据。同时，应立即通过电话等方式向学校网络安全与信息化领导小组办公室报告，不得迟报、谎报、瞒报、漏报。

学校网络安全与信息化领导小组办公室组织研判，认定为一般网络安全事件的，应向学校主要领导和分管领导报告；认定为较大及以上网络安全事件的，应向学校网络安全与信息化领导小组报告，经学校网络安全与信息化领导小组批准后，报省教育网络安全应急办公室。对于人为破坏活动，由学校保卫处确认后报当地公安机关。

4.2 应急响应

网络安全事件应急响应分为 I 级、II 级、III 级、IV 级等四级，分别对应学校特别重大、重大、较大和一般网络安全事件。I 级为最高响应级别。

4.2.1 I 级应急响应和 II 级应急响应

对于特别重大网络安全事件、重大网络安全事件，由上级网络安全应急办公室统一组织应急处置工作，具体要求以上级网络安全应急办公室部署为准。

（1）掌握事件动态

①跟踪事态发展。事发单位应及时主动向学校网络安全与信息化领导小组办公室报告情况，网络安全与信息化领导小组办公室与省教育网络安全应急办公室保持联系，按要求将事态发展变化情况和处置进展情况上报。

②检查影响范围。学校网络安全与信息化领导小组办公室立即了解学校网络和信息系统是否受到事件的涉及或影响，并将有关情况及时报省教育网络安全应急办公室。

③及时汇报情况。学校网络安全与信息化领导小组办公室负责牵头整理上述情况，及时向学校网络安全与信息化领导小组报告；相关重要事项经学校网络安全与信息化领导小组批准后，及时向省教育网络安全应急办公室报告。

（2）处置实施

①控制事态防止蔓延。事发单位以及学校根据事件发生原因，结合相应专项应急预案，采取各种技术措施、管控手段，最大限度阻止和控制事态校内蔓延。

②消除隐患恢复系统。事发单位根据事件发生原因，针对性制定解决方案，备份数据、保护设备、排查隐患。对业务连续性要求高的受破坏网络和信息系统（网站）要及时组织恢复。

③调查取证。事发单位在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极配合学校网络安全与信息化领导小组办公室以及省教育网络安全应急办公室和当地公安机关开展调查取证工作。

④信息发布。学校党委宣传部根据实际，组织网络安全突发事件的应急新闻工作，指导协调相关部门单位开展新闻和舆论引导工作。未经批准，任何部门单位不得发布相关信息。

⑤协调外部支持。处置中需要技术及工作支持的，由学校网络安全与信息化领导小组办公室根据实际情况，商请省教育网络安全应急办公室等单位予以支持。

⑥次生事件处置。对于引发或可能引发其他安全事件的，学校网络安全与信息化领导小组办公室应及时按程序上报。在相关部门应急处置中，学校网络安全与信息化领导小组办公室应积极做好协调配合工作。

4.2.2 III 级应急响应

发生较大网络安全事件，学校网络与信息化领导小组办公室应及时向网络与信息化领导小组汇报，并启动 III 级应急响应。

（1）启动应急指挥。成立应急处置工作组，由分管校领导为组长，学校网络安全与信息化领导小组办公室主任和相关部门单位负责人为成员，必要时可吸纳校外相关部门单位人员参加。应急处置工作组履行事件应急处置工作的领导、指挥、协调职能。

（2）掌握事件动态。学校网络安全与信息化领导小组办公室整理、汇总相关信息，掌握事态发展变化情况和处置进展情况，掌握全校网络和信息系统受到事件涉及或影响的情况，及时向网络安全与信息化领导小组和应急处置工作组报告相关重要事项。领导小组办公室及时形成《教育系统网络安全事件情况报告》（附件 2），经学校网络安全与信息化领导小组批准后，及时报省教育网络安全应急办公室。

（3）实施处置工作。在应急处置工作组的领导下，事发单位根据要求开展应急处置工作，学校网络安全与信息化工作领导小组办公室做好协调工作。

①控制事态防止蔓延。采取各种技术措施、管控手段，最大限度阻止和控制事态蔓延。

②消除隐患恢复系统。事发单位根据事件发生原因，针对性制定解决方案，备份数据、保护设备、排查隐患。对业务连续性要求高的受破坏网络和信息系统（网站）要及时组织恢复。

③调查取证。事发单位在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极配合学校网络安全与信息化领导小组

办公室以及省教育网络安全应急办公室和当地公安机关开展调查取证工作。

④信息发布。学校党委宣传部根据实际，组织网络安全突发事件的应急新闻工作，指导协调相关部门单位开展新闻和舆论引导工作。未经批准，任何部门单位不得发布相关信息。

⑤协调外部支持。应急处置过程中需要校外技术及工作支持的，由学校网络安全与信息化领导小组办公室根据实际，联系校外有关单位予以支持。

⑥次生事件处置。对于引发或可能引发其他安全事件的，事发单位应及时按程序上报。在相关部门应急处置中，学校网络安全与信息化领导小组办公室应积极做好协调配合工作。

4.2.3 IV 级应急响应

发生一般网络安全事件，事发单位应及时向学校网络安全与信息化领导小组办公室报告，经批准后启动 IV 级响应。

（1）启动应急指挥。成立应急处置工作组，由分管校领导为组长，学校网络安全与信息化领导小组办公室主任和相关部门单位负责人为成员，必要时可吸纳校外相关部门单位人员参加。应急处置工作组履行事件应急处置工作的领导、指挥、协调职能。

（2）掌握事件动态。事发单位及时形成《江苏财经职业技术学院网络安全事件情况报告》（附件 3）报学校网络安全与信息化领导小组办公室。学校网络安全与信息化领导小组办公室整

理、汇总相关信息，掌握事态发展变化情况和处置进展情况，掌握全校网络和信息系统受到事件涉及或影响的情况，及时向网络安全与信息化领导小组和应急处置工作组报告相关重要事项。

（3）实施处置工作。在应急处置工作组的领导下，事发单位根据要求开展应急处置工作，学校网络安全与信息化工作领导小组办公室做好协调工作。

①控制事态防止蔓延。采取各种技术措施、管控手段，最大限度阻止和控制事态蔓延。

②消除隐患恢复系统。事发单位根据事件发生原因，针对性制定解决方案，备份数据、保护设备、排查隐患。对业务连续性要求高的受破坏网络和信息系统（网站）要及时组织恢复。

③调查取证。事发单位在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极配合学校网络安全与信息化领导小组办公室开展调查取证工作。

④信息发布。学校党委宣传部根据实际，组织指导协调相关部门单位开展新闻和舆论引导工作。未经批准，任何部门单位不得发布相关信息。

⑤协调外部支持。应急处置过程中需要校外技术及工作支持的，由学校网络安全与信息化领导小组办公室根据实际，联系校外有关单位予以支持。

⑥次生事件处置。对于引发或可能引发其他安全事件的，事发单位应及时按程序上报。在相关部门应急处置中，学校网络安全与信息化领导小组办公室应积极做好协调配合工作。

4.3 应急结束

4.3.1 I 级响应结束和 II 级响应结束

以上级网络安全应急办公室部署为准。

4.3.2 III 级响应结束

经网络安全和信息化领导小组办公室报省教育网络安全应急办同意后，宣布 III 级响应结束，并通报有关情况。

4.3.3 IV 级响应结束

事发单位应急处置完成后向学校网络安全与信息化领导小组办公室报告，经批准宣布 IV 级响应结束。

5 调查与评估

特别重大网络安全事件和重大网络安全事件的调查处理和总结评估工作根据上级有关规定执行。

较大网络安全事件由校网络安全与信息化领导小组办公室组织开展调查处理和总结评估工作，调查评估结果须在提请学校网络安全与信息化领导小组研究同意后上报省教育网络安全应急办公室。

一般网络安全事件由学校网络安全与信息化领导小组办公室会同事发单位组织开展调查处理和总结评估工作。调查评估结果年度网络安全工作总结中具体说明。

网络安全事件的调查处理和总结评估工作应在应急响应结束后5天内完成，应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施，并填报《江苏财经职业技术学院网络安全事件整改报告》（附件4）。

6 预防工作

6.1 日常管理

各部门单位应做好网络安全事件日常预防工作，根据本预案制订完善的应急预案和配套的管理制度，进一步细化应急操作流程，建立完善的应急管理体制。应落实各项防护措施，做好网络安全检查、风险评估和容灾备份，加强信息系统的安全保障能力。

6.2 监测预警和通报

学校应加强网络安全监测预警和通报，及时发现并处置安全威胁。学校网络安全与信息化领导小组办公室应全面掌握全校信息系统（网站）情况，建立全校网络安全监测预警和通报机制，并指导、监督各部门单位及时修复安全威胁，全面排查安全隐患，提高发现和应对网络安全事件的能力。

6.3 应急演练

学校网络安全与信息化领导小组办公室每年组织针对跨部门、跨单位的网络安全事件应急演练，检验和完善预案，提高实战能力，并及时将应急演练情况报省教育网络安全应急办。各部门单位每年至少组织一次应急演练，并将演练情况报送校网络安全与信息化领导小组办公室。

6.4 宣传教育

各部门单位应将网络安全教育作为国家安全教育的重要内容，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传教育。同时，充分利用网络安全宣传周等各种活动形式和传播媒介，开展网络安全基本知识和技能的宣传活动，提高在校师生的网络安全意识。

6.5 工作培训

学校网络安全与信息化领导小组办公室每学期组织一次面向全校相关技术人员的网络安全培训。各部门单位应加强网络安全特别是网络安全事件应急预案的学习，提高网络安全管理和技术人员的防范意识及安全技能。

7 工作保障

7.1 机构和人员

按照“谁主管谁负责”的原则，各部门单位应落实网络安全应急工作责任制，至少配备一名网络安全员，明确具体岗位和人员，建立健全应急工作机制，确保安全事件应急处置科学得当。

7.2 技术保障

学校信息化建设管理处应统筹规划，不断完善网络安全整体方案，积极支持和配合各部门单位加强网络安全技术队伍建设，提高技术监控手段，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支撑工作，确保网络和信息系统的稳定与安全。

建立学校网络安全专家组，为全校网络安全事件的预防和处置提供技术咨询和决策建议，定期开展技术交流活动。

7.3 信息共享与应急合作

加强与省市网络安全职能部门、网络安全专业机构、行业学会（协会）等单位的合作，建立网络安全威胁的信息共享机制和网络安全事件的快速发现和协同处置机制。

7.4 经费保障

学校每年提供专项经费，用于网络安全专家队伍建设、应急技术支撑队伍建设、监测通报、宣传教育培训、预案演练、物资保障等工作开展。

7.5 责任与奖惩

学校对网络安全事件应急管理工作中做出突出贡献的先进集体和个人给予表彰和奖励；对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，依照有关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

8 附则

8.1 预案管理

本预案根据实际情况适时修订。修订工作由学校网络安全与信息化领导小组办公室组织。各部门单位要根据本预案制定或修订本部门单位的网络安全事件应急预案。

8.2 预案解释

本预案由学校网络安全与信息化领导小组办公室负责解释。

8.3 预案实施时间

本预案自印发之日起实施。

江苏财经职业技术学院

2021 年 10 月 8 日

江苏财经职业技术学院校长办公室　　2021 年 10 月 8 日印发

附件 1

信息技术安全事件分类

《信息安全事件分类分级指南》（GB/Z 20986-2007）根据信息技术安全事件的起因、表现、结果等，将信息技术安全事件分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件 7 个基本分类，每个基本分类分别包括若干个子类；根据信息系统重要程度、系统损失和社会影响，将信息技术安全事件划分为 4 个等级。

一、信息技术安全事件分类

1.有害程序事件

有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等 6 个子类。

2.网络攻击事件

网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。网络攻击事件包括拒绝服务攻击事

件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件等 7 个子类。

3.信息破坏事件

信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。信息破坏事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件等 6 个子类。

4.信息内容安全事件

信息内容安全事件是指通过网络发布、传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公共利益的事件。如网站被悬挂反动标识，或有人在网站互动区发布非法内容等。

5.设备设施故障

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件。设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故、和其它设备设施故障等 4 个子类。

6.灾害性事件

灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

7.其他事件

其他事件是指不能归为以上基本分类的信息技术安全事件。

附件 2

教育系统网络安全事件情况报告

部门单位名称：（需加盖公章）事发时间：　　年　月　日

联系人姓名		电子邮箱	
手机		传真	
事件分类	□有害程序事件□网络攻击事件□信息破坏事件 □设备设施故障□灾害事件□其他		
事件分级	□Ⅰ级□Ⅱ级□Ⅲ级□Ⅳ级		
事件概况			
信息系统的基本情况(如涉及请填写)	1.系统名称： 2.系统网址和 IP 地址： 3.系统主管单位/部门： 4.系统运维单位/部门： 5.系统使用单位/部门： 6.系统主要用途： 7.是否定级□是□否，所定级别： 8.是否备案□是□否，备案号： 9.是否测评□是□否 10.是否整改□是□否		

事发单位及事发网络和信息系统功能描述	
事件发生时间、事态发展与处置的简要经过	
事件初步估计的危害和影响（影响程度、影响人数、紧急损失等情况）	
事件原因的初步分析	
已采取的应急措施和效果	

是否需要应急支援及需支援事项和工作建议	
安全负责人意见（签字）	
主要负责人意见（签字）	

附件 3

江苏财经职业技术学院网络安全事件情况报告

部门单位名称：（需加盖公章）事发时间：　　年　月　日

联系人姓名		电子邮箱	
手机		传真	
事件分类	□有害程序事件□网络攻击事件□信息破坏事件 □设备设施故障□灾害事件□其他		
事件分级	□Ⅰ级□Ⅱ级□Ⅲ级□Ⅳ级		
事件概况			
信息系统的基本情况(如涉及请填写)	1.系统名称： 2.系统网址和 IP 地址： 3.系统主管单位/部门： 4.系统运维单位/部门： 5.系统使用单位/部门： 6.系统主要用途： 7.是否定级□是□否，所定级别： 8.是否备案□是□否，备案号： 9.是否测评□是□否 10.是否整改□是□否		

事发单位及事发网络和信息系统功能描述	
事件发生时间、事态发展与处置的简要经过	
事件初步估计的危害和影响（影响程度、影响人数、紧急损失等情况）	
事件原因的初步分析	
已采取的应急措施和效果	

是否需要应急支援及需支援事项和工作建议	
安全负责人意见（签字）	
部门单位主要负责人意见（签字）	

附件 4

江苏财经职业技术学院网络安全事件整改报告

部门单位名称：（需加盖公章）报告时间：　　年　月　日

联系人姓名		手机	
		电子邮件	
事件分类	□有害程序事件□网络攻击事件□信息破坏事件 □设备设施故障□灾害事件□其他		
事件分级	□Ⅰ级□Ⅱ级□Ⅲ级□Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1.系统名称：_ 2.系统网址和 IP 地址： 3.系统主管单位/部门： 4.系统运维单位/部门： 5.系统使用单位/部门： 6.系统主要用途： 7.是否定级□是□否，所定级别：__ 8.是否备案□是□否，备案号：_ 9.是否测评□是□否		

	10.是否整改□是□否
事件发生的最终判定原因（可加页附文字、图片以及其他文件）	
事件的影响与复情况	
事件的安全整措施	
存在问题及建议	
安全负责人意见（签字）	

部门单位主要负责人意见（签字）	